



# High-Performance, Next-Generation Endpoint Security

*The VIPRE Enterprise product line provides you seamless, tightly-integrated security solutions that deliver antivirus and antispyware protection, client firewall, and malicious website filtering technologies that protect against the ever-changing and sophisticated wave of malware in the most comprehensive, highly efficient manner.*

VIPRE Enterprise addresses the pent-up frustration of system administrators over the problems of existing endpoint security solutions, such as bloat, high resource usage, and difficult or poor agent management and deployment.

## A different approach to malware protection

Today, traditional viruses make up only about four percent of the total current malware universe – and are relatively easy to detect and remove. Protecting against the new wave of malware that has emerged over the last five years requires a fundamental shift in how technology is engineered to stay one step ahead of organized cyber criminals. Given the need for increased threat protection, many vendors have responded by retooling their existing antivirus products and adding new layers of antivirus capabilities, rather than building better, more efficient core code. The resulting solutions are bloatware that dramatically impact system performance.

Sunbelt's approach is different. We've translated our years of experience in researching, detecting, and remediating sophisticated malware into the next-generation endpoint protection technology, VIPRE – without building on older generation antivirus engines or other sourced technology components. VIPRE Enterprise is fast, efficient technology in a single, powerful threat engine with low impact on system resources.

## Proprietary anti-malware detection engine uses next-generation technology

At VIPRE's core is an anti-malware engine that merges the detection of viruses, worms, spyware, Trojans, bots, and rootkits into a single efficient and powerful system. VIPRE Enterprise utilizes an advanced technology stack to perform high speed threat scanning to analyze large volumes of information for malware threats in a short period of time with limited performance impact on the end user's PC.

## Real-time monitoring and protection against zero-day threats

VIPRE Enterprise delivers real time monitoring and protection against known and unknown malware threats and leverages a number of proprietary malware detection methods, including dynamic translation (the fastest method of file emulation), heuristics, behavioral analysis and traditional signature-based methods.

VIPRE analyzes the behavior of malware using the following technologies:

- **Active Protection™** – Real-time detection that works automatically inside the Windows kernel, watching for malware and stopping it before it has a chance to execute on a user's system. In addition, administrators can layer their own additional protection rules ("Monitors") to look for specific types of behavior.
- **MX-Virtualization™ (MX-V)** – The built-in MX-V malware analysis technology rapidly analyzes potential malware by observing its behavior in a virtual environment so that malware never actually executes on a user's machine. Because MX-V uses the fastest emulation technique available, Dynamic Translation – it is extremely fast – able to do its work without compromising system performance. The integration of MX-V helps protect users from many unidentified or new variants of malware.
- **Genscan™ and Cobra™ heuristics** – Uses dynamic pattern assessment to determine if a sample is malware.

The combination of all these detection techniques provides an extraordinarily powerful level of real-time protection to endpoints.

## Key Features

**High-performance endpoint security**  
VIPRE delivers fast and memory efficient endpoint security with all the necessary security functionality you need and nothing you don't – ensuring an optimal end user performance experience.

**Powerful, scanning agent technology**  
Superior scanning intelligence that is Checkmark Anti-Virus Desktop certified and VB100 certified. VIPRE delivers high detection rates and fast updates for new exploits.

**Active Protection™**  
Real-time protection of potentially dangerous or bad programs. Dynamic, sophisticated analysis of malware files with advanced behavioral settings.

**MX-V™ technology**  
The built-in MX-V malware analysis technology rapidly analyzes potential malware by observing its behavior in a virtual environment for zero-day threat detection.

**FirstScan™**  
Removes rootkits at the system's boot time and bypasses the Windows operating system, to directly scan certain locations of the hard drive for malware, removing infections where found. Includes native support for 32 and 64-bit Windows platforms.

**Advanced anti-rootkit technology**  
Finds and disables malicious hidden processes, threats, modules, services, files or Alternate Data Streams (ADS) on a user's system.

**Bi-directional firewall**  
Protection against inbound and outbound undesirable activity, with the ability to configure unique rules for applications, ports and system services. Advanced firewall protection is provided with HIPS and IDS.

FEATURES	VIPRE Enterprise	VIPRE Enterprise Premium
Desktop Antivirus & Antispyware	✓	✓
Multi-tiered Site	✓	✓
Single Agent	✓	✓
NAC Support	✓	✓
Desktop Firewall		✓
Host Intrusion Prevention (HIPS)		✓
Intrusion Detection System (IDS)		✓
Malicious URL Filtering		✓
Ad Blocking		✓

*Powerful endpoint protection - you choose which solution is right for your organization*





## Key Features

### Auto-scan removable drives

For self-running media such as USB drives, VIPRE scans autorun.inf and associated files, plus all files on any removable device when it is inserted.

### Easy deployment

Deployment is seamless, featuring an intuitive policy-based user interface with multiple methods to deploy transparently. Agents can be deployed using silent push install (using either WMI or RPC and admin shares), as an MSI file or a self-extracting executable, or auto-deployed through Active Directory or IP ranges and subnets.

### Role-based access control

Granular role-based permissions ensure appropriate access and control for all administrators by region and function.

### Policy-based management

Comprehensive policy creation and management functionality gives you flexibility to control scheduling of scans and all agent options.

### SteadyStream™ Updates

Compact and continuous updates throughout the day, at least 24 updates daily.

### NAC support

As an OESIS-OK Gold Certified product, VIPRE provides seamless integrated control and visibility from the gateway to the desktop when using any OESIS-enabled device, including the market-leading NACs and SSL VPN gateways from vendors such as Cisco, F5, Juniper, Microsoft, SonicWALL, HP, Dell, and TippingPoint.

### Compatibility

VIPRE is compatible with Windows 2000, XP, Server 2003, Vista, Server 2008, Server 2008 R2 and Windows 7, 32- and 64 bit.



## Client firewall and web filtering

The VIPRE Enterprise Premium version delivers client firewall, host-based intrusion prevention (HIPS), network intrusion prevention (NIPS), and an intrusion detection system (IDS) that proactively protects against exploits and zero-day threats.

- **Unique IDS functionality** – Included in VIPRE are pre-defined IDS rules that are updated through VIPRE threat signatures. Administrators also have the ability to write detailed rules based on the Snort® language to complement their own security profile. Rules can be made to block admin-defined inbound or outbound traffic.
- **Boot time firewall** – The Boot Time feature allows administrators to limit access on a desktop to only certain network resources upon loading.
- **Ad blocking** – Automatically block third-party advertisements to reduce web page clutter.
- **Script blocking** – Optionally block Java script, VB scripts, and ActiveX controls.
- **Bad URL blocking** – Bad website blocking that uses the comprehensive ThreatTrack™ malicious URL feeds from SunbeltLabs™.
- **Anti-phishing** – Blocks access to known phishing websites by email or through the web browser.

## Integrated, endpoint email security

VIPRE Enterprise includes comprehensive protection against email viruses, with direct support for Outlook, Outlook Express and Windows Mail; and support for any email program that uses POP3 and SMTP. Additionally, the built-in anti-phishing feature blocks access to phishing websites by stripping out emails that contain phishing links.

## Real-time live threat data integration

VIPRE Enterprise benefits from multiple sources for its threat definition updates with live threat data from SunbeltLabs integrated directly into VIPRE. SunbeltLabs processes tens of thousands of malware samples a day and leverages the following:

- **ThreatNet™** – Sunbelt's user community of hundreds of thousands of thousands of VIPRE consumer users that anonymously send information on possible threats to Sunbelt.
- **Sunbelt CWSandbox™** – The leading automated malware behavior analysis tool for fast and autonomous analysis of large volumes of malware samples.
- **ThreatTrack™** – SunbeltLabs' data feeds that include the latest malicious URLs used to block bad websites and phishing emails.
- **SteadyStream™ Updates** – Provide compact and continuous updates throughout the day – at least once an hour. Incremental updating technology minimizes the size of regular update files, with fast application of updates.

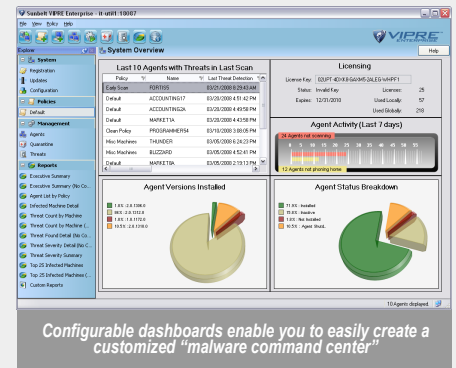
## Centralized management and easy deployment

VIPRE Enterprise is easy to manage and deploy with a simple-to-use platform that provides comprehensive and powerful endpoint protection for all managed desktops and corporate laptops.

- A single agent delivers antivirus and antispysware protection, with client firewall, intrusion prevention, and web filtering in the VIPRE Enterprise Premium version, all handled through a robust central management console.
- Access and control agent deployment, threat database updates, quarantined malware, configuration, agent policies, scan scheduling, and recommended actions to identified malware threats.
- Scalable and flexible multi-site tiering model for large-scale deployments enables distribution of IT workload, allowing regional IT staff to manage local incidents with a consolidated data view of all servers throughout your network. Control multiple physical locations by tiering at the policy level through granular role-based access control or multi-site configuration.

## Reporting

VIPRE's reporting features make it easy for administrators to schedule and customize its library of reports. A report scheduler allows you to easily schedule any report to run at a designated time with the ability to email reports to specified users; simplifying report distribution to management. Additionally, a stand-alone report viewer enables you to provide executive management access to all data in any format without giving them access to the console or database.



Features are subject to change without notice. All products mentioned are trademarks or registered trademarks of their respective companies. Copyright © 2008-2010 Sunbelt Software

vdsFebruary2010

33 N. Garden Ave., Suite 1200, Clearwater, FL 33755 | Tel: 1-888-688-8457 or 727-562-0101 | Fax: 727-562-5199  
www.SunbeltSoftware.com | Email: sales@sunbeltsoftware.com



**Sunbelt Software**  
we keep the bad guys out™